

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE
KRIPTOVALUTE IN PRANJE DENARJA

Ljubljana, april 2020

ŽAN TRŠINAR

IZJAVA O AVTORSTVU

Podpisani Žan Tršinar, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Kriptovalute in pranje denarja, pripravljenega v sodelovanju s svetovalcem prof. dr. Mitjo Kovačem

IZJAVLJAM

1. da sem predloženo delo pripravil samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____

Podpis študenta: _____

KAZALO

UVOD.....	1
1 TEHNOLOGIJA VERIŽENJA BLOKOV.....	2
1.1 Izvorni blok.....	3
1.2 Vozlišča v omrežju Bitcoin	3
1.3 Metode soglasja v tehnologiji veriženja blokov	4
1.3.1 Dokaz o delu	4
1.3.1.1 Primer načina rudarjenja v Ubiq omrežju.....	5
1.3.2 Dokaz o deležu.....	7
1.3.3 Napad na omrežje in problem dvojne porabe.....	7
2 KRIPTOVALUTE.....	9
2.1 Kriptovalute v makroekonomskem okolju	9
2.2 Bitcoin	12
2.3 Ethereum.....	12
2.3.1 ERC-20 standard	12
2.4 Monero	13
2.5 Začetna ponudba kovancev (ICO).....	14
2.5.1 Ocenjevanje vrednosti žetonov/kovancev	15
2.6 Kripto borze.....	16
3 KRIPTOVALUTE IN PRANJE DENARJA	17
3.1 Pranje denarja preko kriptovalut	19
3.2 Pranje kriptovalut.....	21
SKLEP	22
LITERATURA IN VIRI	23

KAZALO SLIK

Slika 1: Enkripcija z javnimi in zasebnimi ključi vs. algoritem zgoščevalne funkcije	2
Slika 2: Veriga blokov v glavni verigi (črna) je najdaljša serija, ki se začne pri izvornem bloku (zelen) in konča pri trenutnem (črn). Sivi bloki so bloki, ki niso del najdaljše verige ter zato niso uporabljeni.....	3
Slika 3: Naprava za rudarjenje (angl. mining rig)	5
Slika 4: Rudarjenje Ethash-DaggerHashimoto algoritma z grafično kartico RX570.....	6

Slika 5: Verjetnost napada na omrežje	8
Slika 6: Različne oblike denarja	10
Slika 7: Neelastičnost ponudbe Bitcoina.....	11
Slika 8: Transakcija BEC žetona.....	13
Slika 9: Skupinski podpis v omrežju Monero	14
Slika 10: Proces pranja denarja po OECD	18
Slika 11: Poenostavljen proces pranja denarja	19
Slika 12: Interaktivno okolje, interakcija kriptovalut in bančnega sistema	20
Slika 13: Omejeno okolje, uporaba kriptovalut kot pretvorba nezakonitih sredstev v zakonite izdelke ali storive	20
Slika 14: Štirje udeleženci in trije sloji mešalnika	21
Slika 15: Nakup orožja z gotovino prek kriptovalut, mešalnika in sintetične identitete.	22

SEZNAM KRATIC

angl. – angleško

BDP – bruto domači proizvod

DAG – (angl. directed acyclic graph); usmerjen aciklični graf

DDoS – (angl. distributed denial-of-service attack); porazdeljena zavrnitev storitve

ECDSA – (angl. elliptic curve digital signature algorithm); algoritem za digitalno podpisovanje z eliptičnimi krivuljami

ECON – (angl. European Commission for Economic Policy); evropska komisija za ekonomsko politiko

ICO – (angl. initial coin offering); začetna ponudba kovancev

IPO – (angl. initial public offering); začetna javna ponudba

KYC – (angl. know your customer); poznavanje ozadja kupca

PV – (angl. present value); sedanja vrednost

SEC – (angl. Securities and Exchange Commission); ameriška komisija za vrednostne papirje in borzo

VC – (angl. venture capital); tvegani kapital

UVOD

Kriptovalute oziroma digitalne valute so se v zadnjem času razširile kot sredstvo na področju monetarne ekonomije, financ, prava in računalništva. »Konkurent ali rešitelj monetarnega sistema?« je vprašanje, ki si ga še danes postavljamo. Njihova uporaba v svetu narašča, vendar po podatkih komisije za ekonomsko politiko (ECON) kljub temu precej zaostaja za širokim denarnim agregatom M3. Seveda je v ozadju predvsem tehnologija veriženja blokov, ki je osnova kriptovalut, med drugim pa s svojo anonimnostjo omogoča prikritje pravega izvora denarja. Tako kriminalnim združbam omogoča vključitev denarja ali premoženja v običajne finančne tokove, zaradi uporabe kot globalnega plačilnega sredstva pa omogoča dostop do sedaj še neznanih trgov (anonimno trgovanje preko spleta).

Zaključna strokovna naloga postavlja naslednja vprašanja: Ali so kriptovalute in njihova tehnologija grožnja ali prihodnost denarnega sistema? Je pranje denarja preko kriptovalut sploh mogoče? Kaj lahko storimo, da preprečimo ali omejimo načine pranja denarja preko kriptovalut.

Zanimalo me je, kakšne postopke se pri pranju denarja uporablja za prikritje pravega izvora denarja, ki je kasneje vrnjen v denarni obtok, poleg tega pa tudi anonimnost v omrežju veriženja blokov.

Moj namen zaključne strokovne naloge je podrobneje spoznati tehnologijo veriženja blokov, kriptovalute in kako jih kriminalne združbe izkoriščajo za svoje potrebe prikritja pravega izvora denarja. Opredeljeni so postopki pranja denarja s kriptovalutami, vzroki pranja denarja ter ukrepi za omejitev oziroma nadzor le-tega.

Cilj naloge je predstaviti tehnologijo, ki poganja kriptovalute ter kako se anonimnost, kot eden izmed osnovnih principov, v nekaterih primerih izkorišča za nezakonite namene.

Pri svoji nalogi bom uporabil deskriptivno metodo, poleg tega pa za dokaz lastništva z rudarjenjem digitalne valute v tehnologiji veriženja blokov kavzalno eksperimentalno metodo (DJS Research Ltd, 2006).

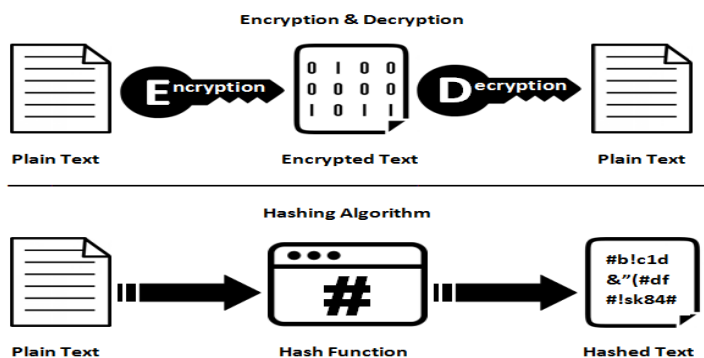
Naloga je razdeljena na tri dele. Prvi del je namenjen tehnologiji veriženja blokov. V drugem delu so opisane kriptovalute, njihov pomen v makroekonomskem okolju in kripto menjalnice. V tretjem delu je interpretirana uporaba kriptovalut za prikritje izvora denarja iz nezakonitih poslov.

1 TEHNOLOGIJA VERIŽENJA BLOKOV

Tehnologija veriženja blokov (angl. blockchain) je nespremenljiva in porazdeljena podatkovna zbirka, v kateri so vpisani podatki, zaščiteni pred neželenim dostopom prek šifriranja (Nakamoto, 2008). Sestavljena je iz dveh terminov: “veriženje” in “blok”. Podatkovno strukturo, ki hrani podatke, imenujemo blok. Vanjo se trajno zapišejo poljubni podatki npr. denarne transakcije, datoteke, podatki o stanju naprav, GPS koordinate, itd. Bloki so organizirani v linearno kronološko zaporedje s časovnim žigom (angl. timestamp), znano tudi kot veriga blokov (Antonopoulos, 2017).

Tehnologija veriženja blokov uporablja algoritem ECDSA (angl. elliptic curve digital signature algorithm) za izračun zasebnega ključa, iz katerega generiramo nove naslove javnega ključa oz. naslova naše kripto denarnice (Antonopoulos, 2017). To pomeni, da lahko pri vsaki transakciji uporabimo nov naslov, na katerega stranka nakaže sredstva, s čimer se zmanjša stopnja sledi (angl. taint) za transakcijami (Koshy, 2013). Pri tem se izkorišča asimetrično šifriranje ter sistem javnih in zasebnih ključev, ki za delovanje potrebuje zgoščevalno funkcijo (angl. hash function). Zgoščevalna funkcija, ki je uporabljena v tehnologiji veriženja, pravi, da je funkcija nepovratna oz. enosmerna. Vhod je poljubno dolgo sporočilo, izhodno sporočilo pa vrne fiksno dolgo binarno vrednost. Vhodno sporočilo je nemogoče najti, če poznamo samo izhodno vrednost. Prav tako je nemogoče najti dve vhodni sporočili, ki tvorita enaka rezultata ob izhodu (Antonopoulos, 2017).

Slika 1: Enkripcija z javnimi in zasebnimi ključi vs. algoritem zgoščevalne funkcije

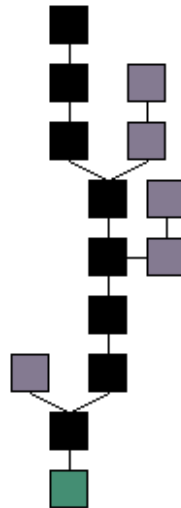


Vir: SSL2Buy (2015).

Evidenco shranjujemo javno, saj lahko vanjo prispeva vsakdo, za nazaj pa je ne more spreminjati (Nakamoto, 2008). Vsak blok ima točno določeno strukturo. Vsebuje metapodatke o bloku in novih transakcijah, podatek o težavnosti rudarjenja bloka, časovnem žigu, naključnem številu kot parametru za vhod zgoščevalne funkcije v postopku iskanja dokazila o delu in zgoščeni vrednosti predhodnega bloka, potrebnega za evidentiranje, kateri blok je predhodni oz. starš trenutnega bloka. Dolžino verige in povezovanje prejšnjega bloka s trenutnim omogočata zadnji dve komponenti

(Antonopoulos, 2017). Tehnologija veriženja blokov je uporabna samo takrat, ko ohrani anonimnost svojih uporabnikov in ko so kopije javne evidence transakcij široko razporejene med udeleženci prek vozlišč. Takrat je spreminjanje zapisov zelo oteženo. Uporaba temelji na poštenosti vseh udeležencev (Nakamoto, 2008).

Slika 2: Veriga blokov v glavni verigi (črna) je najdaljša serija, ki se začne pri izvornem bloku (zelen) in konča pri trenutnem (črn). Sivi bloki so bloki, ki niso del najdaljše verige ter zato niso uporabljeni



Vir: BitcoinWiki (2018).

1.1 Izvorni blok

Izvorni blok (angl. genesis block) je prvi blok v verigi blokov. Sodobne verzije Bitcoina ga štejejo kot blok 0, čeprav so ga zgodnje verzije štele kot blok 1. Izvorni blok je skoraj vedno trdo kodiran (angl. hardcoded) v programsko opremo aplikacij, ki uporabljajo blokovno verigo. Je poseben primer, ker se ne sklicuje na prejšnji blok in proizvede nepovratno funkcijo. (Nakamoto, 2009).

1.2 Vozlišča v omrežju Bitcoin

Vsak uporabnik, ki se poveže z omrežjem Bitcoin, se imenuje vozlišče (angl. node). Vozlišča, ki v celoti preverjajo vsa pravila Bitcoina, se imenujejo polna vozlišča (angl. full node) (Antonopoulos, 2017). Polna vozlišča prenesejo vsak blok in transakcijo celotne verige. Skrbijo za validacijo blokov ter jih preverijo proti pravilom Bitcoina. Spodaj je nekaj pravil:

- Bloki lahko ustvarijo le določeno število Bitcoinov.
- Transakcije morajo imeti pravilne podpise za porabljene Bitcoine.
- Transakcije/bloki morajo biti v pravilni obliki podatkov.
- V eni blokovni verigi izhodne transakcije ni mogoče dvakrat izvesti.

Če blok ali transakcija krši soglasna pravila, potem je blok popolnoma zavrnjen, tudi če vsako drugo vozlišče v omrežju meni, da je veljaven (Nakamoto, 2008). Vozlišče take verige ne sprejme kot ustrezne in je ne pošlje v omrežje ostalim udeležencem. To je ena najpomembnejših značilnosti polnih vozlišč. Pri polnih vozliščih imajo rudarji omejeno moč; lahko samo prerazporedijo ali odstranijo transakcije ob veliki porabi računske moči, pri čemer nastaja problem dvojne porabe (Nakamoto, 2008). Polno vozlišče je obvezno za rudarjenje v omrežju, ni pa obvezno, da polno vozlišče tudi rudari (Antonopoulos, 2017).

Vozlišča, ki imajo različna soglasna pravila, uporabljajo dve različni omrežji. Če spremenimo katerokoli soglasno pravilo, se zgodi delitev omrežja (angl. hard fork), ki ustvari novo digitalno valuto/kovanec (Antonopoulos, 2017).

1.3 Metode soglasja v tehnologiji veriženja blokov

Soglasje v tehnologiji veriženja blokov je postopek dodajanja zapisov transakcij v javno knjigo preteklih transakcij (angl. public ledger). Ta knjiga preteklih transakcij se imenuje veriga blokov, saj vsebuje bloke vseh preteklih transakcij. Poznamo več vrst soglasij, vendar obstajata dve glavni soglasji: dokaz o delu (angl. proof of work) in pa dokaz o deležu (angl. proof of stake) (Mingxiao, Xiaofeng, Zhang, Wang & Qijun, 2017).

Rudarji nenehno dodajajo nove transakcije v nove bloke, ki se dodajo na koncu verige. Ker so bloki zakopani vse globlje in globlje v verigo blokov, jih je vse težje spremeniti ali odstraniti. To povzroči nepovratne transakcije (Antonopoulos, 2017). Nove bloke je nemogoče dodati v verigo brez procesa rudarjenja, ki rešuje matematični problem posameznih blokov. Obstaja več veljavnih rešitev za posamezen blok, vendar za dodajanje bloka v verigo se lahko uporabi le ena izmed rešitev (Antonopoulos, 2017). Vsak udeležen rudar je pri reševanju matematičnega problema bloka nagrajen, saj vsak blok vsebuje zapis, v katerem so naslovi javnega ključa (v tem primeru kripto denarnice rudarjev) upravičeni do nagrade. Ta zapis je znan kot generacijska transakcija in je vedno prva transakcija, ki se pojavi v bloku (Antonopoulos, 2017). Težavnost matematičnega problema se samodejno prilagodi omrežju, ko se število narudarjenih blokov povečuje. Dolžina celotne verige se nanaša na verigo z najbolj kombinirano težavnostjo in ne s tisto z večino blokov (Nakamoto, 2008). To preprečuje, da nekdo verigo razdeli ter tako ustvari veliko število blokov z majhno težavnostjo, ki jo omrežje sprejme kot najdaljšo. Veriga je veljavna samo v primeru, ko so vsi bloki in transakcije v njej veljavni, in le, če se začnejo pri izvirnem bloku. (Nakamoto, 2008).

1.3.1 Dokaz o delu

Posamezni bloki morajo vsebovati dokaz o delu, ki mora biti veljaven. Ta dokaz o delu preverjajo druga vozlišča z veljavno verigo vsakič, ko prejmejo blok (Antonopoulos, 2017).

Slika 3: Naprava za rudarjenje (angl. mining rig)



Vir: Tarring (2018).

Za izvajanje porazdeljenega časovnega strežnika na osnovi med sabo povezanih računalnikov (angl. peer-to-peer) je potreben dokaz o delu (angl. proof of work) (Back, 2002). Dokaz o delu so podatki, ki so dolgotrajni, dragi in kodirani (SHA256, Scrypt, X11, Cryptonight, Ethash), vendar jih tisti, ki izpolnjujejo določene potrebe, lahko preprosto preverijo (Back, 2002). Bitcoin uporablja Hashcashov sistem dokaza o delu (Nakamoto, 2008).

V osnovi je namen preprečiti hekerske napade na serverje (angl. DDoS) tako, da zahteva od uporabnika, da računska moč njegovega procesorja opravi določeno delo (Back, 2002). Dokaz o delu je pravzaprav ena računska moč (procesor) - en glas (Back, 2002). Večinsko odločitev predstavlja veriga, ki ima največji vložek dela. Če večino računske moči nadzorujejo poštena vozlišča (angl. honest nodes), bo poštena veriga rasla najhitreje in bo presegla vse konkurenčne verige (Nakamoto, 2008).

1.3.1.1 Primer načina rudarjenja v Ubiq omrežju

Rudarimo lahko pravzaprav z vsakim računalnikom, ki ima določeno računsko moč. V zadnjem času za rudarjenje uporabljamo predvsem grafične kartice (algoritem Ethash-DaggerHashimoto) ali za to namenjene rudarske naprave, ki uporabljajo zmogljiva čipovja (ASIC), ki so zmožna računsko moč uporabljati 100.000-krat hitreje kot trenutno najboljši procesorji na trgu. Take naprave praviloma rudarijo algoritem SHA-256, ki ga uporablja Bitcoin (Bhaskar & Kuo Chuen, 2015).

Če želimo rudariti algoritem Ethash-DaggerHashimoto, ki ga uporabljajo nekatere digitalne valute kot npr. ethereum, ubiq in drugi, uporabimo preprosto programsko kodo, s katero se pridružimo bazenu rudarjev (angl. mining pool).

```
setx GPU_FORCE_64BIT_PTR 0
```

```
setx GPU_MAX_HEAP_SIZE 100
```

```
setx GPU_USE_SYNC_OBJECTS 1
```

```
setx GPU_MAX_ALLOC_PERCENT 100
```

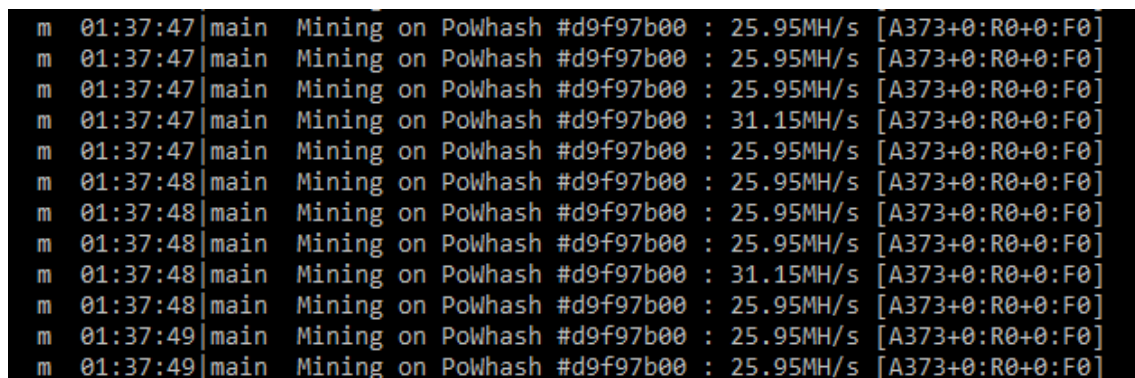
```
setx GPU_SINGLE_ALLOC_PERCENT 100
```

```
ethminer.exe --farm-recheck 200 -G -S ubiq-eu.maxhash.org:10008 -FS ubiq-  
us.maxhash.org:10008 -SP 1 -O
```

Wallet ID : worker ID

S to programsko kodo bo računalnik uporabil računsko moč grafične kartice in tako obremenil delovni pomnilnik (angl. random access memory – RAM) naše grafične kartice.

Slika 4: Rudarjenje Ethash-DaggerHashimoto algoritma z grafično kartico RX570



```
m 01:37:47|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:47|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:47|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:47|main Mining on PoW hash #d9f97b00 : 31.15MH/s [A373+0:R0+0:F0]  
m 01:37:47|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:48|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:48|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:48|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:48|main Mining on PoW hash #d9f97b00 : 31.15MH/s [A373+0:R0+0:F0]  
m 01:37:48|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:49|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]  
m 01:37:49|main Mining on PoW hash #d9f97b00 : 25.95MH/s [A373+0:R0+0:F0]
```

Vir: lastno delo.

Seveda pa je naše rudarjenje oz. nagrada za rudarjenje odvisna tudi od zmogljivosti naših komponent ter usmerjenega acikličnega grafa (angl. directed acyclic graph – DAG). Usmerjeni aciklični graf je usmerjen graf brez usmerjenih ciklov. Pravzaprav je množica vozlišč in zbirka usmerjenih povezav, tako da vsaka povezava povezuje urejen par točk (Buterin, 2013).

Specifičen je za vsak kovanec, ki uporablja Ethash-DaggerHashimoto algoritem. V primeru Ethereum, Dagger temelji na zmerno povezanem usmerjenem acikličnem grafu, ki deluje tako, da ustvari usmerjeni aciklični graf z desetimi stopnjami, vključno s korenom in skupno vrednostjo 2^{25-1} (Buterin, 2013). Računanje dokaza o delu zahteva podmnožice fiksne vrednosti. Ta vir se imenuje DAG in se spremeni vsakih 30.000 blokov (100-urno okno, imenovano obdobje ali epoch) (Buterin, 2013). V preprostem prevodu to pomeni, da ne bomo mogli rudariti z grafičnimi karticami, ki imajo premalo delovnega pomnilnika skozi čas.

1.3.2 Dokaz o deležu

Dokaz o deležu je predlagana alternativa dokazila o delu, ki je krožila v krogih skupnosti Bitcoin od leta 2011 (Bitcointalk, 2011). Pri dokazu o delu algoritem nagrajuje rudarje, ki rešujejo matematične probleme s ciljem potrditve transakcij in ustvarjanja novih blokov. V nasprotju pa se pri dokazu o deležu oblikovalec novega bloka izbere na determinističen način, odvisen od njegovega deleža, ki ga ima v lasti (King & Nadal, 2012). To pomeni, da v sistemu dokaza o deležu ni nobenega nagrajevanja, tako da rudarji prevzemajo transakcijske stroške generacijskih transakcij. Rudarji se v takem sistemu imenujejo kovači (angl. forgers) (King & Nadal, 2012).

Nekateri trdijo, da bi metode, ki temeljijo na samem dokazu o delu, lahko povzročile nizko varnost omrežja v kriptovaluti s povišanjem težavnosti omrežja oz. manjšo nagrado ob večjem številu narudarjenih blokov, prav tako pa težavo predstavlja vse višja poraba elektrike pri sistemu dokaza o delu, pri čimer se spopademo z dilemo tragedije skupnih virov (Bitcointalk, 2011). Ta nastane, ko ima več oseb dostop do skupne dobrine, pri tem pa pravila uporabe ne omejujejo njihovih osebnih interesov, da bi preprečila pretirano izrabo skupnega dobrega. To lahko pripelje do uničenja skupnega dobrega (Hardin, 1968).

1.3.3 Napad na omrežje in problem dvojne porabe

Večinski napad (običajno označen z 51 % ali >50 % napad) je napad na omrežje, ki zahteva več kot 50 % računske moči omrežja. Napadalec omrežju predloži transakcijo, ki jo plača trgovcu, medtem ko zasebno rudari zasebno verigo, v kateri je vključena dvojna poraba transakcije. Po čakanju n potrditev trgovec pošlje izdelek. Če napadalec na tej točki najde več kot n blokov, sprosti zasebno verigo in ponovno dobi poslane kovance nazaj. V večini primerov so vse kriptovalute ranljive za napad z več kot 50 % računske moči. Nekateri, kot na primer IOTA, pa so ranljivi tudi za napade s 33 % računske moči, saj uporabljajo drugačno tehnologijo veriženja blokov, tako imenovani tangle (DAG), kjer vsaka transakcija predstavlja blok. Vsak blok potrdi sebe tako, da sledi usmerjenemu toku in potrdi dve drugi naključni transakciji.

Možnost napada oz. dvojne porabe lahko izračunamo z naslednjo enačbo:

$$q_z = \begin{cases} 1, & \text{if } p \leq q \\ (q/p)^z, & \text{if } p > q \end{cases} \quad (1)$$

p = verjetnost poštenega vozlišča, da najde naslednji blok

q = verjetnost napadalca, da najde naslednji blok

q_z = verjetnost napadalca, da kdaj ujame število z blokov že v verigi

Glede na predpostavko, da $p > q$, verjetnost pada eksponentno ob večanju števila blokov, ki jih mora napadalec dohiteti ob podaljševanju verige.

Sedaj bomo pogledali, kako dolgo mora prejemnik nove transakcije čakati potrditev, preden bo dovolj prepričan, da napadalec transakcije ne more spremeniti. Predvidevamo, da je pošiljatelj napadalec, ki želi, da bi prejemnik verjel, da je plačal, nato pa preklopi transakcijo, ki se mu vrne po preteku določenega časa. Prejemnik bo opozorjen, ko se to zgodi, vendar pošiljatelj upa, da bo prepozno. To stori tako, da na paralelni verigi ustvari alternativno verzijo svoje transakcije. Prejemnik čaka, dokler transakcija ni dodana v blok ter v število z blokov za njim, ne pozna pa števila nezaupljivih blokov v verigi, ki jih je napadalec ustvaril. Napadalčev potencialni napredek števila blokov je Poissonova porazdelitev s pričakovano vrednostjo:

$$\lambda = z \frac{q}{p} \quad (2)$$

Da bi dobili verjetnost, da bi napadalec še lahko dohitel verigo, množimo Poissonovo porazdelitev (2) za vsak napredek, ki ga naredi, z verjetnostjo, da ujame verigo:

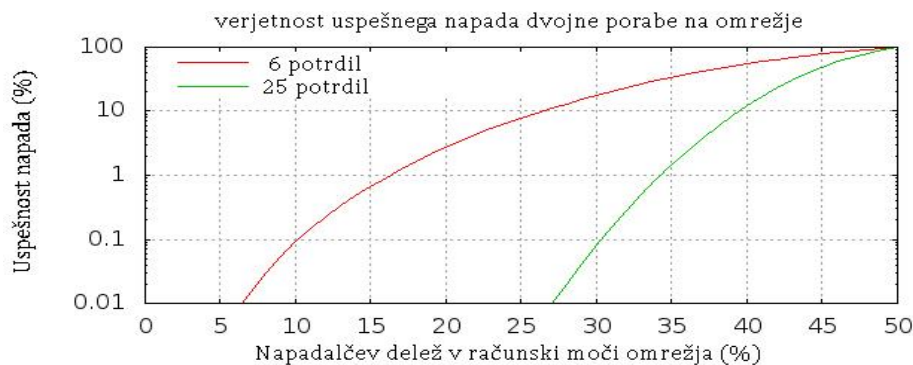
$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} * \begin{cases} (q/p)^{(z-k)}, & \text{if } k \leq q \\ 1, & \text{if } k > q \end{cases} \quad (3)$$

Enačbo (3) poenostavimo, da se izognemo neskončnemu repu porazdelitve.

$$1 - \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} * (q/p)^{(z-k)} \quad (4)$$

Iz zgornje enačbe (4) vidimo, da verjetnost eksponentno pada z večanjem števila blokov z (Nakamoto, 2008).

Slika 5: Verjetnost napada na omrežje



Vir: prirejeno po Pabr Technologies (2014).

Večinski napad ni bil nikoli uspešno izveden v omrežju Bitcoin, vendar je bil uspešen pri nekaterih manjših kriptovalutah. Težava se pojavi pri združevanju rudarjev v bazene rudarjev (BitMEX Research, 2019).

2 KRIPTOVALUTE

Kriptovalute so digitalna ali virtualna valuta oz. deviza, ki služi kot digitalna oblika menjalnega sredstva pri trgovanju. Gre za proces pretvorbe čitljivih podatkov v skoraj nerešljivo kodo, ki omogoča sledenje prenosov virtualnega denarja/deviz. Kriptovalute olajšajo prenos sredstev med dvema stranema, hkrati pa zagotavljajo varno transakcijo z uporabo javnih in zasebnih ključev (Nakamoto, 2008). Kriptovalute niso vezane na posamezno državo in njeno centralno banko. Ti prenosi se izvajajo z minimalnimi stroški obdelave transakcij, so mednarodni in uporabnikom omogočajo, da se izognejo plačilom provizij, ki jih banke in finančne institucije zaračunavajo (Antonopoulos, 2017).

V preteklem desetletju je prišlo do velikega porasta kriptovalut na internetu. Do danes jih poznamo že več kot 1000 (Xena Exchange, 2019).

Kriptovalute zagotavljajo določeno raven anonimnosti. Zaradi ravni anonimnosti, ki jo ponujajo, pa so kriptovalute pogosto povezane z nezakonitimi posli in storitvami, zlasti na globokem spletu (Telegraph Reporters, 2018).

2.1 Kriptovalute v makroekonomskem okolju

Denar se je v zgodovini pojavljal v različnih oblikah menjalnega sredstva. Predmeti, ki so bilo izdelani predvsem iz žlahtnih kovin (baker, srebro, zlato) ali pa tudi drugih surovin (sol, idr.), so obstajali kot naravni denar (European Central Bank, 2015). Naturalnemu je sledil reprezentativni denar. To so bili bankovci, ki jih je bilo mogoče zamenjati za določeno količino zlata ali srebra (European Central Bank, 2015). Sodobni denar, ki ga uporabljajo sodobna gospodarstva, pa temelji na zaupanju. Temu pravimo fiduciarni denar. Tak denar je zakonito plačilno sredstvo in ga izda centralna banka (European Central Bank, 2015). Za razliko od reprezentativnega denarja ga ni mogoče zamenjati za vnaprej določeno količino zlata. Papir, ki se uporablja za bankovce, sam po sebi nima vrednosti, vendar se uporablja v zameno za blago in storitve, ker ljudje zaupajo centralni banki, da bo tudi v prihodnje ohranjala njegovo vrednost (European Central Bank, 2015). Fiduciarni denar bi izgubil splošno sprejemljivost kot menjalno sredstvo, če bi banki pri ohranjanju vrednosti denarja spodletelo (European Central Bank, 2015). Euro kot valuta se lahko uporablja kot zakonito plačilno sredstvo v prostoru evropske monetarne unije in tudi drugje, z uporabo valutnih tečajev.

Centralne banke posojajo denar poslovnim bankam, s čimer vplivajo na tok denarja in kreditov v gospodarstvu. V večini gre za izposojanje iz centralnobančne rezerve za potrebe zelo kratkoročnih likvidnostnih potreb. Centralne banke tudi določajo zelo kratkoročne obrestne mere in s tem povpraševanje poslovnih bank po centralnobančnih rezervah ter imajo tako nadzor nad količino zunanjega denarja (European Central Bank, 2015).

Centralne banke imajo tudi vpliv pri programih nakupa vrednostnih papirjev, ki predstavljajo eno od možnih oblik kvantitativnega rahljanja, in s tem posredno ohranjanja stabilne vrednosti denarja (European Central Bank, 2015).

V praksi denar definiramo s tremi funkcijami (Claeys, Demertzis & Efsthathiou, 2018):

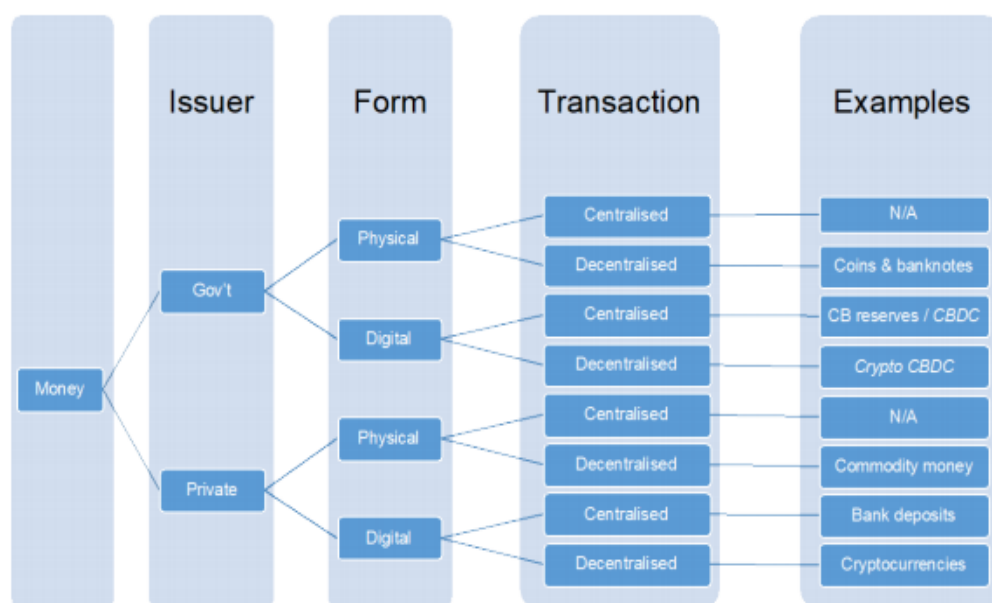
- merilo vrednosti; skupno merilo vrednosti blaga in storitev, s katerimi trguje gospodarstvo in je izraženo s ceno,
- menjalno sredstvo; sprejet za plačilo blaga in storitev, poplačilo dolgov,
- hranilec vrednosti; kot način shranjevanja bogastva z namenom prenosa kupne moči iz sedanjosti v prihodnost.

Preden pa se posvetimo kriptovalutam, si pogledjmo pogoje, ki so potrebni za uspeh določene oblike denarja, in kako se kriptovalute razlikujejo od različnih vrst denarja.

Osredotočimo se na tri glavna merila (Bech & Garratt, 2017):

- izdajatelj: državni ali zasebni,
- oblika: fizična ali digitalna,
- poravnavna transakcije: centralizirana ali decentralizirana.

Slika 6: Različne oblike denarja



Vir: Claeys, Demertzis & Efsthathiou (2018).

Kriptovalute predstavljajo obliko denarja, ki doslej ni bila na voljo. So izdane zasebno, kar sicer ni novo, vendar za razliko od bančnih depozitov kriptovalute niso obveznost in jih tudi ni mogoče unovčiti (Claeys, Demertzis & Efsthathiou, 2018). So digitalne, podobne elektronskemu denarju, ki ga izdajajo centralne banke. Tako kot elektronski denar so tudi kriptovalute fiduciarni denar (Claeys, Demertzis & Efsthathiou, 2018).

Poravnava transakcij poteka na decentraliziran način. Izmenjave kriptovalut so peer-to-peer (P2P). Za uporabo kriptovalut je potrebna digitalna denarnica, pri zamenjavi z drugimi valutami pa so vključeni posredniki (kripto borze) (Claeys, Demertzis & Efsthathiou, 2018). Novost kriptovalut je v izvedljivosti digitalnih peer-to-peer transakcij.

Prednosti tega so decentralizacija, zasebna izdaja in digitalna oblika kriptovalut.

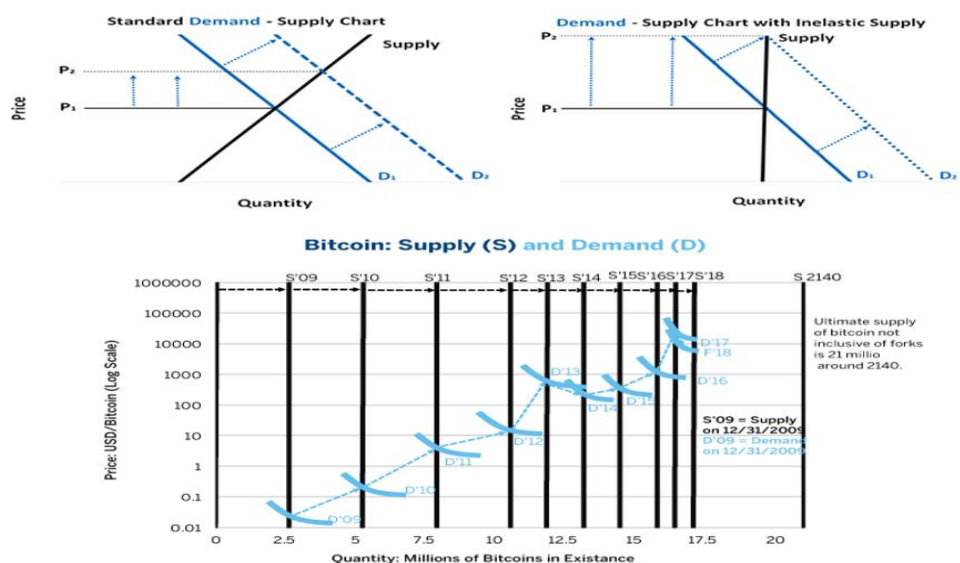
Decentralizacija zagotavlja skoraj popolno anonimnost transakcij, kar omogoča zasebnost. To lahko pomeni, da kriptovalute olajšajo transakcije, povezane z nezakonitimi dejavnostmi ali davčno utajo (Claeys, Demertzis & Efsthathiou, 2018). Kriptovalute so veliko bolj nagnjene k takšnim dejavnostim v primerjavi z gotovino, saj imajo možnost opravljanja velikih transakcij (Claeys, Demertzis & Efsthathiou, 2018). Tehnologija veriženja blokov je v primerjavi s centraliziranimi sistemi tudi manj občutljiva na zlonamerne napade in tako zagotavlja zanesljivo knjigo preteklih transakcij (Bech & Garratt, 2017).

Digitalna oblika kriptovalut in nezavezanost katerikoli oblasti omogočata resnično globalno in lahko dostopno valuto, ki lahko olajša globalno trgovino (Claeys, Demertzis & Efsthathiou, 2018).

O zasebni izdaji ne odloča nobena politična institucija, temveč algoritem, ki ga podporniki kriptovalut vidijo kot način, kako se izogniti diskrecijskim odločitvam, ki bi lahko vodile do previsoke inflacije (Claeys, Demertzis & Efsthathiou, 2018). Pri transparentnih kriptovalutah je mogoče denarno politiko predvideti iz algoritma.

Izogibanje diskrecijskim odločitvam pomeni, da izgubimo fleksibilnost pri soočanju s krizami zaradi neelastičnosti ponudbe denarja. To razloži volatilnost kriptovalut (Putnam & Norland, 2018).

Slika 7: Neelastičnost ponudbe Bitcoina



Vir: Putnam & Norland (2018).

Danes centralne banke zagotavljajo elastično ponudbo valut za izpolnitev mandatnega cilja - cenovne stabilnosti. Centralnim bankam se tako omogoča uporabo mnogih instrumentov za doseg cilja (vpliv na kratkoročne obrestne mere, nakup sredstev, idr.) (Claeys, Demertzis & Efsthathiou, 2018).

V nadaljevanju je predstavitev nekaterih kriptovalut: bitcoin, ethereum in monero.

2.2 Bitcoin

Prva decentralizirana kriptovaluta, kjer je bila uporabljena tehnologija veriženja blokov, je bil bitcoin (Champagne, 2014). Ustanovljen je bil leta 2008 ob objavi študije z naslovom *Bitcoin: A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008). Identiteta skrivnostnega avtorja ali skupine avtorjev pod tem psevdonimom še danes ni znana. Bitcoin obljublja nižje transakcijske stroške od tradicionalnih plačilnih mehanizmov spletnega plačevanja in se upravlja prek decentraliziranega organa, za razliko od centraliziranih valut, ki jih izdaja država oz. centralna banka. Fizični bitcoini ne obstajajo, saj so celotno omrežje, transakcije in stanja v denarnici shranjeni v vozliščih. Vse to je objavljeno v javni knjigi transakcij. Kljub temu, da ni zakonito plačilno sredstvo, je bitcoin postal zelo priljubljen in je sprožil začetek uporabe drugih virtualnih valut, ki jih imenujemo alternativni kovanci (angl. altcoins) (Frankenfield, 2019).

2.3 Ethereum

Tako kot Bitcoin, je Ethereum porazdeljena javna blokovna mreža. Ethereum je zasnoval ustanovitelj Vitalik Buterin leta 2013, razvoj pa je bil finančno podprt z javno prodajo kovancev. Čeprav obstajajo nekatere pomembne tehnične razlike med njima, se bitcoin in ether predvsem razlikujeta po namenu in zmožnosti. Bitcoin ponuja vsak-z-vsakim (angl. peer-to-peer) elektronski denarni sistem, ki omogoča spletno plačevanje z bitcoini, medtem ko se ethereum osredotoča na poganjanje decentraliziranih aplikacij v smislu superračunalnika (angl. ethereum virtual machine). Za razliko od Bitcoina so rudarji v omrežju Ethereum nagrajeni z etherom. Ether uporabljajo razvijalci aplikacij za plačevanje transakcijskih stroškov in storitev v omrežju (Ethereum, 2015).

2.3.1 ERC-20 standard

ERC-20 standard opredeljuje skupen seznam pravil za vse žetone ethereuma (angl. tokens), ki jih je potrebno upoštevati, kar pomeni, da morajo razvijalci natančno napovedati, kako bodo novi žetoni delovali v sistemu ethereum (Ethereum, 2015). Vpliv, ki ga ima ERC-20 standard na razvijalce, je огromen, saj projektov ni potrebno ponavljati vsakič, ko se sprosti nov žeton. Namesto tega so zasnovani tako, da so združljivi z novimi žetoni, pod pogojem, da se ti žetoni držijo pravil. Obstajajo tudi drugi standardi, kot so ERC-223, ERC-721 idr. (Ethereum, 2015).

Čeprav pošiljatelj pozna javni naslov prejemnika, prejemnik naslova ne more pregledati v javni knjigi transakcij. Transakcije v omrežju Monero so zaupne in prikrite, za razliko od omrežja Bitcoin, kjer je knjiga transakcij javna in so se zato v preteklosti pojavljale težave z anonimnostjo (Koshy, 2013). Ob vsaki transakciji v omrežju Monero se ustvari nov naslov prejemnika in pošiljatelja. Tako ni mogoče izslediti naslovov s pomočjo analize transakcij (Monero, 2014).

Monero je prav tako edinstven zaradi uporabe kriptografskih skupinskih podpisov. V omrežju Monero namesto ene osebe skupina posameznikov odpre transakcijo, s čimer ustvari skupinski podpis, vendar samo ena oseba v tej skupini poseduje kovanec monero.

Slika 9: Skupinski podpis v omrežju Monero



Vir: CryptoNote Technology (2014).

Te lastnosti kovanca monero so postale priljubljene predvsem pri skupini, ki želi anonimnost - črni trg globokega spleta. Zaradi omogočene anonimnosti se povečuje število nezakonitih uporabnikov (Greenberg, 2017). Po pričakovanju Monerovih razvijalcev se bodo kovanci nedvomno uporabljali tudi pri drugih nezakonitih načinih, kot so izsiljevalski virusi (angl. ransomware), vendar pa naj bi se kljub temu večinoma uporabljali za bolj nedolžne oblike finančne zasebnosti, kot je zaupnost našega premoženja ali nakupov knjig v represivnih režimih (Greenberg, 2017).

2.5 Začetna ponudba kovancev (ICO)

Podjetja in posamezniki se vse bolj nagibajo k začetnim ponudbam kovancev (angl. initial coin offering - ICO) kot načinu zbiranja kapitala ali sodelovanja pri naložbenih priložnostih (U.S. Securities and Exchange Commision, 2018a). Medtem ko lahko ta digitalna sredstva in tehnologija predstavljajo nova in učinkovita sredstva za opravljanje finančnih transakcij, po drugi strani povečujejo tveganje goljufije in manipulacije, ker so trgi za ta sredstva manj regulirani od tradicionalnih kapitalskih trgov (U.S. Securities and Exchange Commision, 2018b). Pravni status začetnih ponudb kovancev je v večini nedefiniran. V najboljšem primeru se žeton ne prodaja kot finančno sredstvo, temveč kot digitalna dobrina (U.S. Securities and Exchange Commision, 2018b).

Začetna ponudba kovancev (ICO) je v nekaterih pogledih podobna začetni javni ponudbi (IPO), vendar pa za razliko od IPO-ja, kjer vlagatelji pridobijo lastništvo v podjetju, ICO-ji zagotavljajo vlagateljem žetone, ki imajo neko vrednost ali omogočajo dostop do določenih funkcij izdelka/platforme (Gajjaria, 2017). Prav tako ne moremo primerjati

ICO-jev in tradicionalnega modela tveganega kapitala (VC). Tradicionalni tvegani kapital dovoljuje investicijo samo akreditiranim vlagateljem, ki imajo dolgotrajen proces primerne skrbnosti (angl. due diligence) (Gajjaria, 2017). Medtem pa ICO-ji omogočajo vsem vlagateljem, da sodelujejo v postopku financiranja in jim omogočijo, da svoje vložene žetone zamenjajo na različnih platformah v druge valute. To omogoča start-upom hitrejšo pridobivanje denarja v tehnologiji veriženja blokov in vlagateljem več načinov izstopa iz investicije (Gajjaria, 2017).

2.5.1 Ocenjevanje vrednosti žetonov/kovancev

Kripto-žetoni niso niti valuta in ne vrednostni papir (U.S. Securities and Exchange Commission, 2018a). Lahko vključujejo vidike obeh in imajo značilnosti, ki so povsem nove. Glede na te vidike se sprašujemo, kako ugotovimo, koliko so žetoni vredni.

Pogledali si bomo nekaj osnovnih modelov vrednotenja.

Če so žetoni valuta, potem velja Fischerjeva enačba kvantitativne teorije o denarju (poenostavljeno)(5), pri kateri je vrednost transakcij v obdobju (T) enaka količini denarja v obtoku (M), pomnoženi s hitrostjo kroženja denarja (V).

$$T = MV \quad (5)$$

Zgornja enačba (5) pomeni: če je izdanih M število žetonov, bo imel vsak žeton vrednost $\frac{T}{MV}$ (Conley, 2017).

Če upoštevamo, da so žetoni vrednostni papirji, potem mora biti njihova vrednost enaka sedanji vrednosti (angl. present value – PV)(6). Če vzamemo enostaven primer, potem imetnik žetona pričakuje naslednje tokove plačil; $\pi = \{\pi_1, \pi_2, \dots, \pi_t\}$. Recimo, da so oportunitetni stroški kapitala r %, kar pomeni, da je stopnja donosa r , ki jo je mogoče zaslužiti pri najboljši razpoložljivi naložbi. Potem mora biti vrednost žetona naslednja:

$$\sum_{t=1}^T (1 - r)^t * \pi_t \quad (6)$$

Če bi se žeton prodal za katero koli drugo ceno, bi bila to boljša ali slabša naložba. Povpraševanje in cena bi se torej premaknili navzgor ali navzdol, kjer bi žetoni vrnilo točno r % (Conley, 2017).

Hipoteza učinkovitosti trga kapitala pravi, da je najboljši napovedovalec jutrišnje cene današnja cena (7). Trenutna cena vrednostnega papirja ali valute mora vključevati vse javno razpoložljive informacije, ki bi lahko nanjo vplivale.

$$p_t = E(p_{t-1}) \quad (7)$$

Denimo, da je današnja cena nižja od pričakovane jutrišnje. Tako bi lahko danes kupili in jutri prodali z dobičkom. Ker je to na voljo vsem, bi današnja cena poskočila na enako jutrišnjo pričakovano ceno. Prvič, ko postanejo nove informacije javne, se tako prihodnja

kot trenutna cena prilagodita. Če podjetje patentira nov izum, se pričakuje, da se bo dobiček povečal ter se bo cena prilagodila novi, višji sedanji vrednosti. To ne upošteva tveganja in predpostavlja, da bodo dobički vrednostnega papirja konstantni. Dodati moramo tudi diskontne stopnje prihodnjih cen z oportunitetnimi stroški kapitala (Conley, 2017).

V nekaterih primerih udeleženci ne sledijo racionalnemu vedenjskemu vzorcu. V prostoru veriženja blokov so kripto-žetoni novi in privlačni. Delnice in vrednosti papirji pa so stari in dolgočasni. Mogoče je, da je udeleženec pripravljen plačati več za sodelovanje v podjetju, prek začetne ponudbe kovancev (ICO) kot prek začetne javne ponudbe (IPO). To pomeni, da je vrednost žetonov (8):

$$p = ? \quad (8)$$

Z drugimi besedami, ne vemo. V kolikor lahko najdemo pravila, ki opisujejo sistematično, predvidljivo, čeprav neracionalno vedenje, so ekonomske teorije še uporabne. Vendar je to v novih situacijah/tehnologijah težko, tudi npr. v tehnologiji veriženja blokov in začetnih ponudbah kovancev (Conley, 2017).

2.6 Kripto borze

Kripto izmenjevalnice oz. borze delujejo na podoben način kot banke. Postopek verifikacije (angl. know your customer – KYC) postopek je obligatoren za vse uporabnike reguliranih kripto borz. Ta obsega kopijo osebnega dokumenta, potrdilo o bivanju in sliko z osebnim dokumentom. Denar nakažemo na račun kriptoborze, s katerim lahko kupujemo in prodajamo kriptovalute (Bitcoin Wiki, 2017). Izmenjava se opravi z oddajo nakupnih ali prodajnih naročil, ki jih borza izvrši. Nakupna naročila so ponudbe za nakup določene kriptovalute v zameno za drugo valuto. Prodajna naročila so ponudbe za prodajo kriptovalute v zameno za drugo fiduciarno valuto (Bitcoin Wiki, 2017).

Če platforma ponuja trgovanje z digitalnimi sredstvi, ki so vrednostni papirji, in deluje kot borza, kot je opredeljeno v zveznih zakonih ZDA, se mora platforma registrirati pri SEC (angl. Securities and Exchange Commission) kot borza vrednostnih papirjev. Tak proces je namenjen zaščiti vlagateljev in preprečevanju goljufivih in manipulativnih trgovskih praks (U.S. Securities and Exchange Commission, 2018b).

Izmenjava fiduciarnega denarja v kriptovalute poraja nekatera vprašanja v zvezi z goljufijami pri vračanju denarja. Natačneje, načine plačila, kot so kreditne kartice in PayPal, je mogoče preklicati do 90 dni po izvedbi transakcije. Nasprotje pa je bitcoin - ko enkrat porabimo bitcoine, jih ne moremo več dobiti nazaj (razen z napadom na omrežje, ki je opisan v poglavju 1.3.3). Tako je trgovanje z mehko valuto, kot so PayPal in kreditne kartice, podvrženo tveganju povratne bremenitve po tem, ko je kriptovaluta že poslana s kripto borze. Kupec lahko sproži povratno bremenitev tako, da prijavi

sumljivo aktivnost na računu oz. da je nekdo zlorabil račun ter opozori na bremenitev, ki je ni izvedel ali pa tudi je (Bitcoin Wiki, 2017).

V letu 2010 se je zgodilo prav to. Dve glavni kripto borzi (Bitcoin Market in Mt. Gox) sta bili oktobra 2010 prizadeti z veliko količino transakcij preko PayPal, kjer so posamezniki ali skupine posameznikov uporabili ukradene PayPal račune za financiranje njihovih kripto računov in za nakup bitcoinov (Bitcointalk, 2010). To je povzročilo zamrznitev PayPal računa Mt.Goxa in začasno ukinitvev registracije novih uporabnikov na kripto borzi. Ta zamrznitev je v tistem času povzročila začasno likvidnostno težavo za bitcoin, saj je postalo težje zamenjati fiduciarne valute v bitcoine (Bitcointalk, 2010).

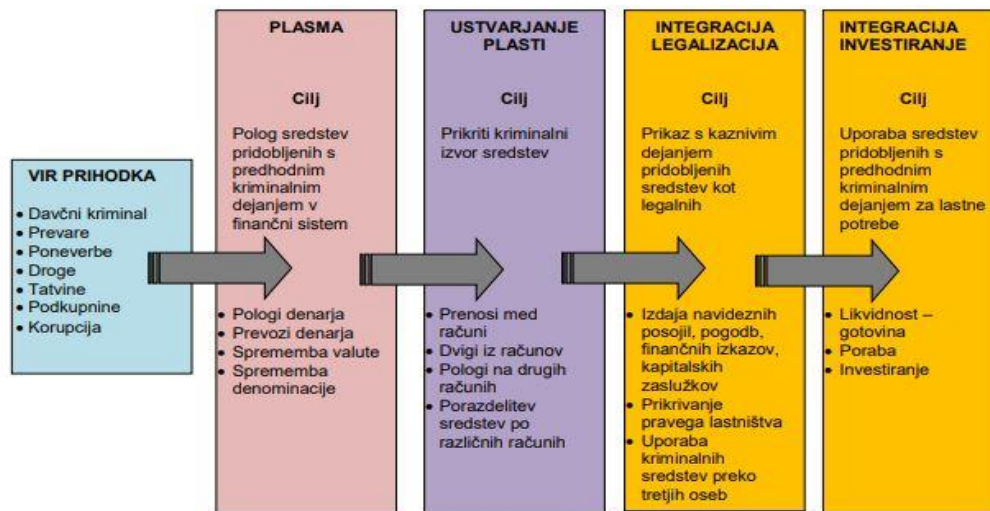
3 KRIPTOVALUTE IN PRANJE DENARJA

Dobički, ki so posledica nezakonitih dejavnosti, ki jih pridelajo kriminalne mreže, kot so trgovina z ljudmi ali drogami, tihotapljenje in nedovoljene igre na srečo, resno ogrožajo gospodarski sistem in javno varnost. Ti dobički zagotavljajo finančna sredstva za kriminalne združbe in teroristične organizacije ter zmanjšujejo davčne prihodke (McDowell & Novis, 2001). Pranje denarja je proces, s katerim prikrijemo povezavo med nezakonitim virom dobička in izvorno kriminalno dejavnostjo (International Monetary Fund, 2014). Pojav kompleksnih finančnih instrumentov in globalnega mreženja s tehničnim razvojem ter uporabo interneta ponuja doslej neznane poti pranja denarja. Zato ni presentljivo, da je bilo v letu 2009 iz nezakonitih virov opranih kar 1,6 bilijarde dolarjev sredstev, kar znaša 2,6 % svetovnega BDP (United Nations Office on Drugs and Crime, 2011).

Poznamo tri faze pranja denarja (Lamberger, 2009):

- prenos denarja/plasma/plasiranje sredstev (angl. placement; sorting and refining) v finančni sistem države. Gotovinski prenos, kjer se gotovina preko prenosa denarja prenaša preko državnih meja s tihotapljenjem, in brezgotovinski prenos, kjer se sredstva prenašajo preko finančnih institucij, menjalnic.
- prikrivanje izvora denarja/ustvarjanje plasti/legalizacija denarja (angl. layering) poteka preko tujih družb, finančnih institucij in z nakupom nepremičnin v tujini. Če je prikritje uspešno in legalizirano ter se izvor sredstev zakrije, se sredstva lahko prenesejo v matično državo. Pri pranju denarja prihaja do določenega stroška. Tako združbe po pranju denarja dobijo manj denarja kot pred pranjem, vendar je prikazan, kot da je pridobljen z legalnimi posli.
- vključitev/integracija/vračanje opranega denarja (angl. intergration) je vključitev sredstev v gospodarstvo ali ponovno investiranje v kriminalno dejavnost. Po legalizaciji se denar vrne iz tujine v matično državo s transakcijami preko tujih družb ali bank. Sredstva se po vrnitvi v matično državo investirajo v nove legalne ali ilegalne posle, dobiček pa se opere v naslednjem krogu pranja denarja.

Slika 10: Proces pranja denarja po OECD



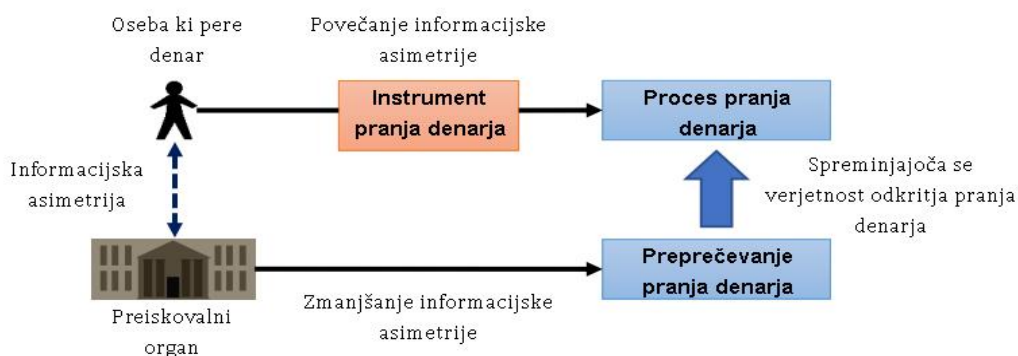
Vir: Špilak (2016).

Pranje denarja je kaznivo dejanje in je po 2. členu Zakona o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1), Ur. l. RS, št. 68/16 in 81/19 opredeljeno kot »katerokoli ravnanje, s katerim se prikriva izvor denarja ali drugega premoženja, pridobljenega s kaznivim dejanjem in vključuje:

- zamenjavo ali kakršenkoli prenos denarja ali drugega premoženja, ki izvira iz kaznivega dejanja;
- skrivanje ali prikrivanje prave narave, izvora, nahajanja, gibanja, razpolaganja, lastništva ali pravic v zvezi z denarjem ali drugim premoženjem, ki izvira iz kaznivega dejanja.«

Uspešnost pranja denarja je odvisna tudi od informacijske asimetrije med pralci denarja in preiskovalnimi organi. Dejavnosti pranja denarja imajo dve ključni značilnosti: nezakonnost in prikrivanje (Masciandaro, 1999). Za ponovno uporabo nezakonito pridobljenih sredstev dejavnosti ne smejo povzročati suma, poleg tega pa morajo nastati iz legitimih virov. Zato je cilj pranja denarja zajeti tok gotovine na način, ki preprečuje kakršno koli povezavo z osnovnimi kriminalnimi dejavnostmi (United Nations Office on Drugs and Crime, 2005). V ekonomskem smislu je to prenos kupne moči v dejansko kupno moč, tako da zmanjšamo tveganje za inkriminacijo. Proces vzpostavitve te asimetrije informacij se imenuje postopek pranja denarja in se izvaja z instrumenti pranja denarja. Preiskovalni organi za preprečevanje, odkrivanje in preiskovanje pranja denarja, se imenujejo uradi za preprečevanje pranja denarja. Cilj uradov je zmanjšati asimetričnost informacij med pralci denarja in preiskovalnimi organi (Becker, 1968). Bolj ko so ti učinkoviti, težje je storilec kaznivih dejanj uspešno izvesti postopek pranja denarja in se s tem okoristiti. Z večjim tveganjem povečajo možnosti pregona in obsodbe (Becker, 1968).

Slika 11: Poenostavljen proces pranja denarja



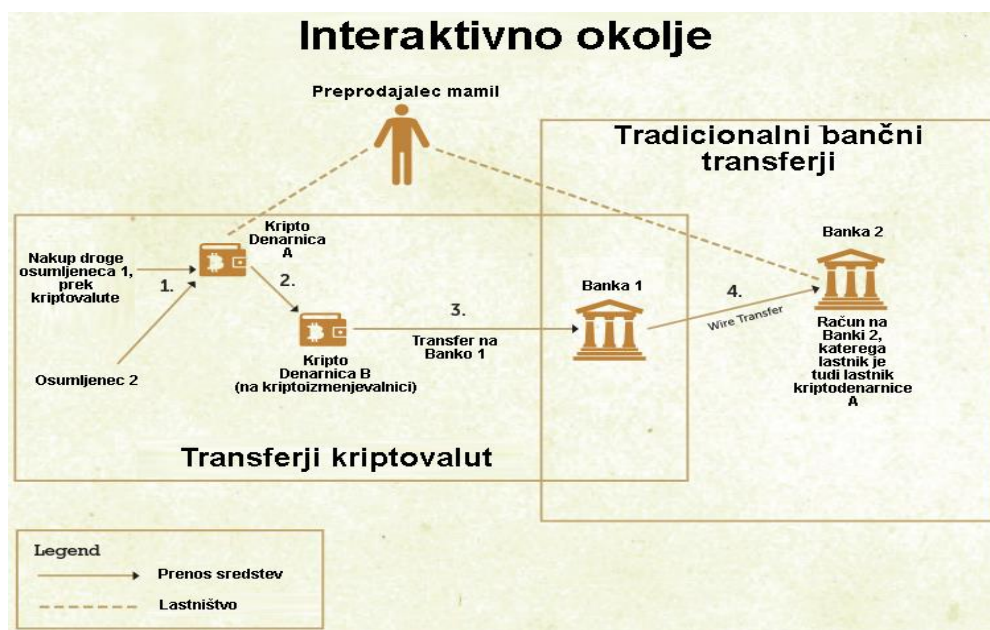
Vir: prirejeno po Brenig, Accorsi & Muller (2015).

3.1 Pranje denarja preko kriptovalut

Interaktivno okolje je tisto, v katerem se kriptovalute križajo s tradicionalnim bančnim sistemom. Na sliki 12 je izpostavljena interakcija med bančnim sistemom in kriptovaluto. Prikazuje primer, kako tehnologija veriženja blokov služi prikritju sredstev, povezanih z nezakonitim prenosom premoženja.

Ta scenarij vključuje preprodajalca z drogami, ki uporablja kriptovalutno denarnico, kripto izmenjevalnice in medbančna plačila, s čimer si izplača prihodek iz kaznivih dejanj. Preprodajalec proda drogo, ki je plačana s kriptovaluto. Kriptovaluta se prenese na naslednjo denarnico, ki je na kripto izmenjevalnici, katera kasneje pretvori kriptovaluto v fiduciarno valuto in se prenese na bančni račun. Preiskovalec bi lahko opazoval račun, ki je odprt na banki 1, vendar ne ve, da je bančni prenos izveden iz kripto izmenjevalnice. Zato je potrebno, da se preiskovalec zaveda, da prenosi, ki prihajajo iz večjih, preverjenih in bolj zaupljivih kripto izmenjevalnic, veljajo za uveljavljene, zaupljive in regulirane. Pri banki 2 preiskovalci ne bi mogli odkriti povezave s kriptovalutami in bi videli samo medbančni transfer. Preiskovalec ne bi mogel vzpostaviti povezave med bančnim računom na banki 2 in kriptodenarnico A (Mari, Warrack & Real, 2016).

Slika 12: Interaktivno okolje, interakcija kriptovalut in bančnega sistema

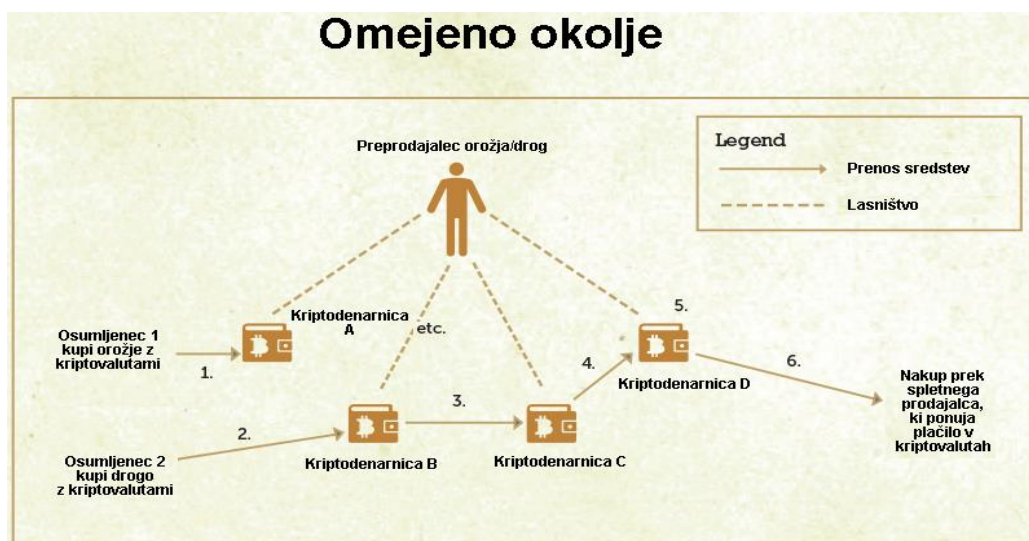


Vir: prirejeno po Mari, Warrack & Real (2016).

V omejenem okolju vse transakcije potekajo izven tradicionalnega bančnega sistema in so vidne le znotaj blokovne verige.

V sliki 13 je preprodajalec orožja/drog sposoben zbrati denar (transakcija 1 in 2) in celotno prodajo svojih nezakonitih storitev (transakcija 3 in 4) poravnati na blokovni verigi. V transakciji 5 preprodajalec kupi izdelke ali storitve preko spletnega prodajalca, ki sprejema kriptovalute. Preiskovalci v takih primerih teh transakcij niti morejo opaziti (Mari, Warrack & Real, 2016).

Slika 13: Omejeno okolje, uporaba kriptovalut kot pretvorba nezakonitih sredstev v zakonite izdelke ali storitve



Vir: prirejeno po Mari, Warrack & Real (2016).

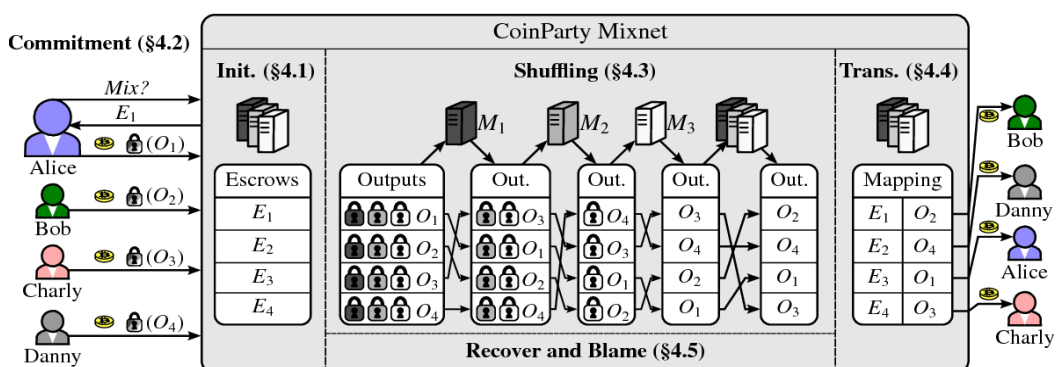
3.2 Pranje kriptovalut

Tako kot računi v tradicionalnem bančnem sistemu so bančne denarnice dovzetne za omejitve glede vodenja evidenc in prepoznavanja lastnikov računa. V obeh primerih lahko oseba uporabi sintetične identitete ali pooblaščenke za odpiranje računov. Sintetična identiteta je identiteta, ki v resničnem življenju ne obstaja. Z drugimi besedami, oseba se ni nikoli rodila (Mari, Warrack & Real, 2016). Torej se razlikuje od kraje identitete resnične osebe. Zaradi svojega obstoja v digitalnem okolju je tudi transakcijam v blokovni verigi težje slediti prek anonimizatorjev IP naslovov. Prav tako je težje slediti kriptovalutam, ki gredo skozi "mešalnik" (angl. tumbler, mixer), ki izmenja kriptovaluto s »čistejšimi« kovanci. Medtem ko IP anonimizatorji prikrijejo dejansko lokacijo lastnika denarnice, mešalniki pripomorejo k prikrivanju izvora sredstev (Mari, Warrack & Real, 2016).

Slika 12 opisuje scenarij, v katerem so udeleženi štirje udeleženci in trije sloji mešalnika. V resničnem scenariju pa so raziskovalci v Rusiji poskušali identificirati sumljive transakcije v blokovni verigi bitcoina. V tem primeru je bil en bitcoin prenos razdeljen na 98 slojev in plačan drugim imetnikom kriptodenarnic (Sat in drugi, 2016).

V srednjem nizu transakcij mešalnik izmenja in opravi več transakcij tako, da zakrije sled »umazanih« kovancev. Takim kovancem je kasneje težje slediti po transakcijski sledi in zaporedju dogodkov (Sat in drugi, 2016). Mešalniki združujejo kovance s kovanci ostalih udeležencev in se zmešajo s »čistimi« kovanci. Mešalnik pošlje transakcije z različnimi količinami v druge kriptodenarnice, ki jih nadzoruje in tako simulira omrežne transakcije. Na primer, uporabnik, ki pošlje v mešalnik en bitcoin, lahko prejme več manjših transakcij skozi čas. Tako en bitcoin večkrat izmenja več različnih naslovov (Sat in drugi, 2016).

Slika 14: Štirje udeleženci in trije sloji mešalnika

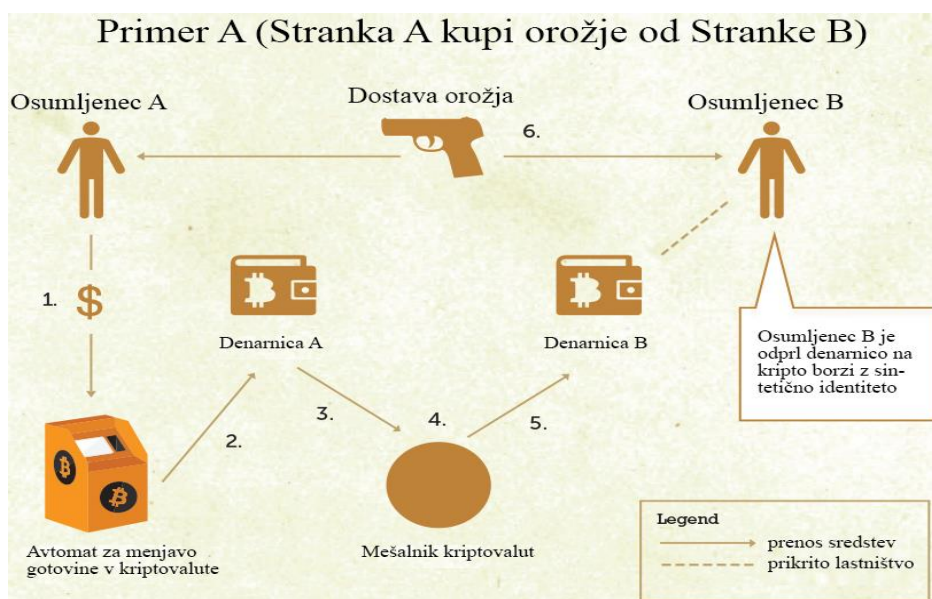


Vir: Ziegeldorf, Matzutt, Henze, Grossmann & Wehrle (2016).

Z uporabo sintetične identitete, mešalnikov in gotovine, ki jo izmenjamo prek kriptovalutnih bankomatov v zameno za kriptovalute (ki nimajo KYC postopka), se

organom pregona močno oteži delo. Spletne transakcije potekajo preko prikritih oz. anonimiziranih IP naslovov (prikazano na sliki 15).

Slika 15: Nakup orožja z gotovino prek kriptovalut, mešalnika in sintetične identitete



Vir: prirejeno po Mari, Warrack & Real (2016).

Na sliki 15 osumljenec A pretvori gotovino v kriptovaluto in si jo nakaže v svojo denarnico A. Sredstva v denarnici A se mešajo z mešalnikom kriptovalut in so poslana v denarnico B za prikritje izvora prvotne gotovinske transakcije. Po prejemu plačila osumljenec B dostavi orožje osumljenecu A. S takšnimi metodami lahko organizirane kriminalne mreže in teroristi izvajajo nezakonite posle zunaj reguliranega finančnega sistema (Mari, Warrack & Real, 2016).

SKLEP

Zaključna strokovna naloga raziskuje delovanje tehnologije veriženja blokov ter naslavlja vprašanja o pomenu kriptovalut in procesu pranja denarja preko njih. V teoretičnem delu sem raziskal, kako različni avtorji interpretirajo tehnologijo veriženja blokov in pomen kriptovalut v makroekonomskem okolju. V praktičnem delu sem izvedel poskus pranja denarja preko kriptovalut in dokazal, da je prikrivanje izvora denarja preko kriptovalut izvedljivo. Opisal sem tudi različne scenarije, kako je mogoče prikriti izvor denarja.

Kriptovalute so lahko prihodnost digitalnega denarnega sistema. Monetarna politika kriptovalut je že vnaprej opredeljena z algoritmom, ki onemogoča napačne odločitve, ki bi vodile do previsoke inflacije. V primerjavi s tradicionalnim bančnim sistemom kriptovalute edine omogočajo transparentnost, varnost in anonimnost transakcij. To je pomembna prednost predvsem pri mednarodnih prenosih denarja, predstavlja pa tudi dobro izhodišče za delovanje brezgotovinske družbe in globalne trgovine. Kriptovalute

so privlačne tudi zaradi decentraliziranega načina digitalne poravnave transakcij, ki omogočajo prenos sredstev brez posrednika in s tem nizke transakcijske stroške.

Kot vsaka tehnologija pa ima tudi tehnologija veriženja blokov nekatere pomanjkljivosti. Prikrivanje izvora denarja je skozi zgodovino potekalo na različne načine. Z razvojem tehnologije se hkrati razvija tudi pranje denarja. Kriptovalute to omogočajo na doslej še neuporabljene načine, katerim se bodo morali organi pregona in zakonodajalci prilagoditi. Kljub splošni domnevi, da je izsleditev kriptovalut nemogoča, je to možno preko analize sledenja kripto transakcij in preko vzorca transakcij. Vendar pa ima tudi ta analiza svoje omejitve.

Anonimnost kripto transakcij je odvisna od posamezne kriptovalute in načina šifriranja javnih in zasebnih ključev, pa tudi od glavne knjige transakcij, če je ta javna ali zasebna. Težava anonimnosti se pojavi pri več transakcijah v določen času iz ene kripto denarnice. Tako lahko določimo vzorec transakcij in na ta način razkrijemo IP naslov uporabnika kripto denarnice. Trenutno je nemogoče oceniti vrednost denarja, opranega preko kriptovalut.

Pranje denarja preko kriptovalut je možno omejiti. Potrebno je definirati, kaj sploh kriptovalute so. Transparentnost in reguliranost kriptomenjalnic je prioriteta, KYC postopki bi morali biti obvezujoči za vsakršno transakcijo izven menjalnice. Prav tako bi moral biti KYC postopek opravljen tudi na avtomatu pri nakupu kriptovalute preko določenega zneska. Šele z definiranimi pojmi se lahko sestavi zakon, potreben za regulacijo in transparentnost kriptovalut.

Kriptovalute morajo premagati tri glavne ovire, da bi postale širše uporabljene. Postati morajo legitimno menjalno sredstvo v očeh vlad in regulatorjev. Cene morajo biti stabilne in ne pretirano volatilne, kot so v tem trenutku, kar prinaša prednosti tako trgovcem kot tudi potrošnikom. Imeti morajo globalni doseg v plačilnem trgu, kjer se je potrebno povezati z ponudniki plačilnih kartic, kot so Visa, Mastercard, idr.

V prihodnjem desetletju ne bi presenetilo, če bi kakšna kriptovaluta nepričakovano nastala tudi s pomočjo katere od centralnih bank. Tako vlade, banke kot tudi ponudniki bančnih kartic se vse bolj nagibajo k tako imenovani "brezgotovinski" družbi. Države z zgodovinsko močnimi bančnimi sistemi se ozirajo proti kriptovalutam. Vprašanje pa je, katera država bo prva sprejela prednosti kriptovalut in premagala vse trenutne ovire.

LITERATURA IN VIRI

1. Antonopoulos, M. A. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. Sebastopol: O'Reilly Media.
2. Back, A. (2002, 1. avgust). *Hashcash - A Denial of Service Counter-Measure*. Pridobljeno 7. maj 2018 iz <http://www.hashcash.org/hashcash.pdf>

3. Bech, M. & Garratt, R. (2017). *Central bank cryptocurrencies*. Basel: Bank for international settlements, Quaterly Review.
4. Becker, G. (1968). Crime and Punishment: An Economic Approach. *The Journal of Political Economy*, 76(2), 169–217.
5. Bhaskar, N. & Kuo Chuen, D. (2015). Chapter 3 - Bitcoin Mining Technology. V *Handbook of Digital Currency* (str. 45–65). Cambridge: Academic Press.
6. Frankenfield, J. (2019, 29. oktober). *Bitcoin Definition*. V Investopedia. Pridobljeno 4. april 2020 iz <https://www.investopedia.com/terms/b/bitcoin.asp>
7. Bitcointalk. (2010, 14. oktober). *PayPal dropped MtGox*. Pridobljeno 5. maj 2018 iz <https://bitcointalk.org/index.php?topic=1419.65;imode>
8. Bitcointalk. (2011, 11. julij). *Proof of stake instead of proof of work*. Pridobljeno 10. maj 2018 iz <https://bitcointalk.org/index.php?topic=27787.0>
9. BitMEX Research. (2019, 24. maj). *The Bitcoin Cash Hardfork – Three Interrelated Incidents*. [objava na blogu]. Pridobljeno 10. maj 2020 iz <https://blog.bitmex.com/the-bitcoin-cash-hardfork-three-interrelated-incidents/>
10. Block Chain. (2018, 28. oktober). V *Bitcoin Wiki*. Pridobljeno 5. maj 2018 iz https://en.bitcoin.it/wiki/Block_chain
11. Brenig, C., Accorsi, R. & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. *ECIS 2015 Completed Research Papers*. Münster: European Research Centre for Information Systems. Pridobljeno 10. maj 2018 iz https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1019&context=ecis2015_cr
12. Buterin, V. (2013, december). *Dagger: A Memory-Hard to Compute, Memory-Easy to Verify Script Alternative*. Pridobljeno 7. maj 2018 iz <http://www.hashcash.org/papers/dagger.html>
13. Buterin, V. & Wood, G. (2014, 1. september). *A Next-Generation Smart Contract and Decentralized Application Platform*. Pridobljeno 15. maj 2018 iz <https://github.com/ethereum/wiki/wiki/White-Paper>
14. Champagne, P. (2014). *The Book Of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*. Austin: E53 Publishing.
15. Claey's, G., Demertzis, M. & Efstathiou, K. (2018). *Cryptocurrencies and monetary policy*. Brussels: European Parliament.
16. Conley, J. P. (2017, 6. junij). *Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings*. Nashville: Vanderbilt University Department of Economics Working Papers. Pridobljeno 1. junij 2018 iz https://pdfs.semanticscholar.org/16d3/e5bc47bea18c1d4056ebbe548acff3aeef4f.pdf?_ga=2.258536330.187193691.1586895056-293929330.1586895056
17. Currency exchange. (2017, 28. september). V *Bitcoin Wiki*. Pridobljeno 5. maj 2018 iz https://en.bitcoin.it/wiki/Currency_exchange
18. Difference Between Hashing and Encryption. (2017, 28. september). V *SSL2Buy*. Pridobljeno 5. maj 2018 iz <https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption>

19. DJS Research Ltd. (2006, 6. julij). *What is Casual Research*. Pridobljeno 12. maj 2018 iz <http://www.marketresearchworld.net/content/view/799/64/>
20. ERC token standards. (2015). V *Ethereum*. Pridobljeno 12. maj 2018 iz <https://docs.ethhub.io/built-on-ethereum/erc-token-standards/erc20/>.
21. European Central Bank. (2015, 24. november). *What is Money*. Pridobljeno 5. marec 2020 iz https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.sl.html
22. Gajjaria, A. (2017, 16. avgust). IPOs, meet ICOs, Initial coin offerings offer funding alternatives. *Deloitte*. Pridobljeno 23. marec 2018 iz <https://www2.deloitte.com/us/en/pages/financial-services/articles/icos-offer-funding-alternatives.html>
23. Greenberg, A. (2017, 25. januar). *Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire*. *Wired*. Pridobljeno 5. april 2018 iz <https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/>
24. Hardin, G. (1968, 13. December). The Tragedy of the Commons. *Science* 162, 1243–1248.
25. International Monetary Fund. (2014). *The IMF and the Fight Against Money Laundering and the Financing of Terrorism*. Pridobljeno 5. april 2018 iz <http://www.imf.org/external/np/exr/facts/pdf/aml.pdf>
26. King, S. & Nadal, S. (2012, 12. August). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. Pridobljeno 12. maj 2018 iz https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf?_ga=2.84327440.809630090.1587421226-1031688879.1587421226
27. Koshy, D. (2013). *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. University Park: Pennsylvania State University.
28. Lamberger, I. (2009). *Gospodarski Kriminal*. Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.
29. Mari, J., Warrack, P. & Real, L. (2016). *When Two Worlds Collide*. Miami: ACAMS Today. Pridobljeno 10. maj 2018 iz <https://www.acamstoday.org/when-two-worlds-collide/>
30. Masciandaro, D. (1999, maj). Money Laundering: the Economics of Regulation. *European Journal of Law and Economics*, 7(3), 225–240.
31. McDowell, J. & Novis, G. (2001). The Consequences of Money Laundering and Financial Crime. *Economic Perspectives* 6 (2), 6–10.
32. Mingxiao, D., Xiaofeng, M., Zhang, Z., Wang, X. & Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Banff, AB, Canada: IEEE.
33. Monero How. (2014). *A low-level explanation of the mechanics of Monero vs Bitcoin in plain English*. Pridobljeno 2. maj 2018 iz <https://www.monero.how/how-does-monero-work-details-in-plain-english>
34. Nakamoto, S. (2008, 31. oktober). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Pridobljeno 6. maj 2018 iz <https://bitcoin.org/bitcoin.pdf>

35. Nakamoto, S. (2009, 3. januar). *MIT/X11 software license, Line 1613*. Pridobljeno 10. 3 2018 iz <https://sourceforge.net/p/bitcoin/code/133/tree/trunk/main.cpp#l1613>
36. Putnam, B. & Norland, E. (2018). *An In-Depth Look at the Economics of Bitcoin*. Chicago: CME Group.
37. Orcutt, M. (2018, 1. marec). *Ethereum's smart contracts are full of holes*. MIT Technology Review. Pridobljeno 5. maj 2018 iz <https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/>
38. Pabr Technologies. (2014, 9. september). *Bitcoin's centralized endgame, and how to avoid it*. Pridobljeno 18. maj 2018 iz <http://www.pabr.org/bcendgame/bcendgame.en.html#>
39. PeckShield Inc. (2018, 22. april). *ALERT: New batchOverflow Bug in Multiple ERC20 Smart Contracts* [objava na blogu]. Pridobljeno 20. maj 2018 iz <https://blog.peckshield.com/2018/04/22/batchOverflow/>
40. Ring signatures: Untraceable payments (2015). V *CryptoNote Technology*. Pridobljeno 10. maj 2018 iz <https://cryptonote.org/inside>
41. Sat, D. M., Krylov, G. O., Evgenyevich, K., Bezverbnyi, Kasatkin, A. B. & Kornev, I. A. (2016, 20. januar). Investigation of Money Laundering Methods through Cryptocurrency. *Journal of Theoretical and Applied Information Technology*, 83, 244–254.
42. Špilak, M. (2016). *Izbira programske rešitve za preprečevanje pranja denarja in financiranja terorizma*. Ekonomska fakulteta. Ljubljana: Univerza v Ljubljani. Pridobljeno 10. marec 2020 iz <http://www.cek.ef.uni-lj.si/magister/spilak5003.pdf>
43. Tarring, S. (2018, 2. februar). *Building a 12 GPU Mining Rig with Sapphire RX570's & Simple Mining OS*. [objava na blogu] Pridobljeno 18. maj 2018 iz <https://medium.com/redhivemining/building-a-12-gpu-mining-rig-with-sapphire-rx570s-simple-mining-os-62af17299d8e>
44. Telegraph Reporters. (2018, 17. avgust). *What is cryptocurrency, how does it work and why do we use it?* Pridobljeno 1. september 2018 iz <https://www.telegraph.co.uk/technology/0/cryptocurrency/>
45. Town, S. (2018, 25. april). *BatchOverflow Exploit Creates Trillions of Ethereum Tokens, Major Exchanges Halt ERC20 Deposits*. Pridobljeno 5. maj 2018 iz <https://cryptoslate.com/batchoverflow-exploit-creates-trillions-of-ethereum-tokens/>
46. U.S. Securities and Exchange Commission. (2018a, 27. marec). *Spotlight on Initial Coin Offerings (ICOs)*. Pridobljeno 8. april 2018 iz <https://www.sec.gov/ICO>
47. U.S. Securities and Exchange Commission. (2018b, 7. marec). www.sec.gov. Pridobljeno 8. april 2018 iz <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>
48. United Nations Office on Drugs and Crime. (2005, 1. december). *Model legislation on money laundering and financing of terrorism*. Vienna: United Nations Office on Drugs and Crime. Pridobljeno 5. marec 2018 iz

- <https://www.unodc.org/documents/money-laundering/2005%20UNODC%20and%20IMF%20Model%20Legislation.pdf>
49. United Nations Office on Drugs and Crime. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. Vienna: United Nations Office on Drugs and Crime. Pridobljeno 23. januar 2018 iz http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
50. Xena Exchange. (2019, 6. avgust). *Exploring the Digital Landscape: How Many Cryptocurrencies Are There?* [objava na blogu] Pridobljeno 5. marec 2020 iz <https://xena.exchange/blog/exploring-the-digital-landscape-how-many-cryptocurrencies-are-there/>
51. Ziegeldorf, J. H., Matzutt, R., Henze, M., Grossmann, F. & Wehrle, K. (2016). *Secure and Anonymous Decentralized Bitcoin Mixing*. Aachen: Communication and Distributed Systems (COMSYS), RWTH Aachen University. Pridobljeno 10. maj 2018 iz <https://www.henrikziegeldorf.de/wp-content/papercite-data/pdf/ziegeldorf2016secure.pdf>